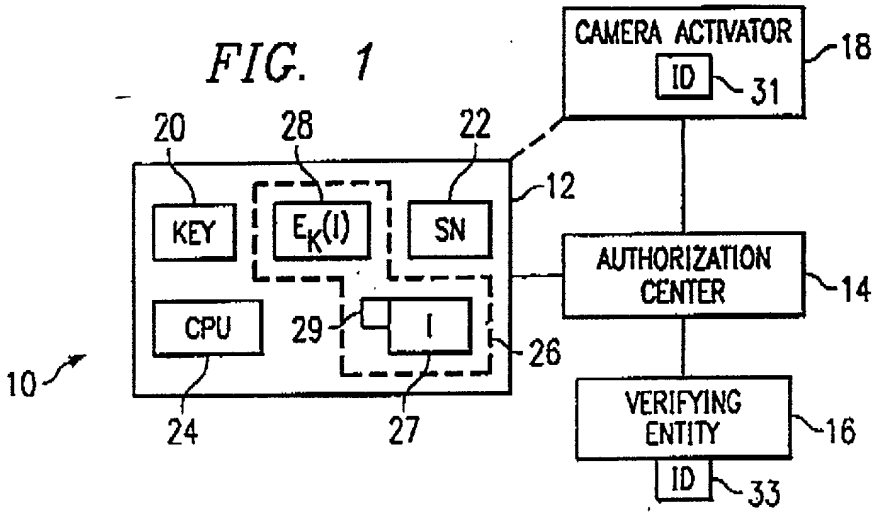
FIG. 1



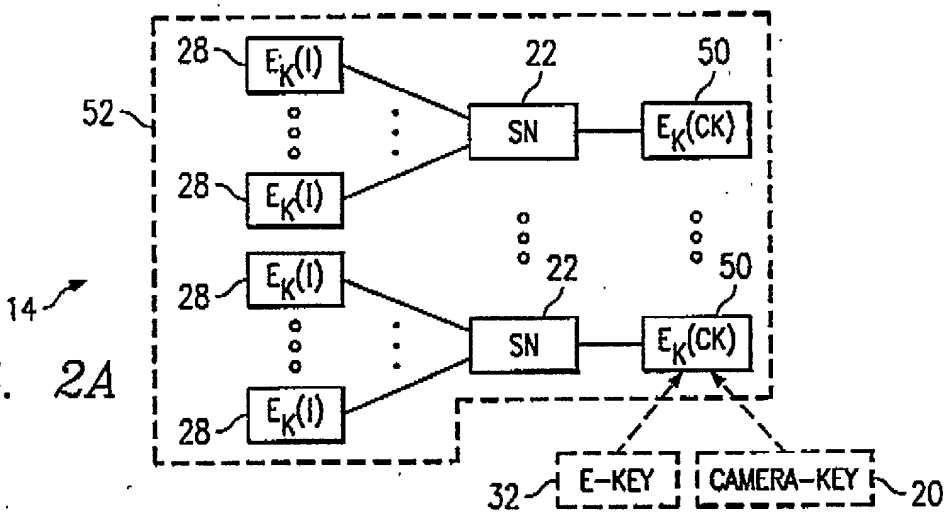


FIG. 2A

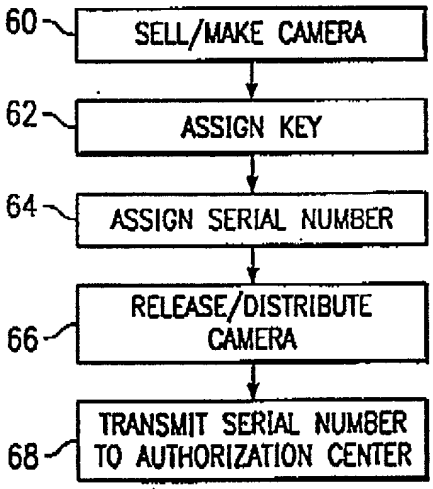


FIG. 3

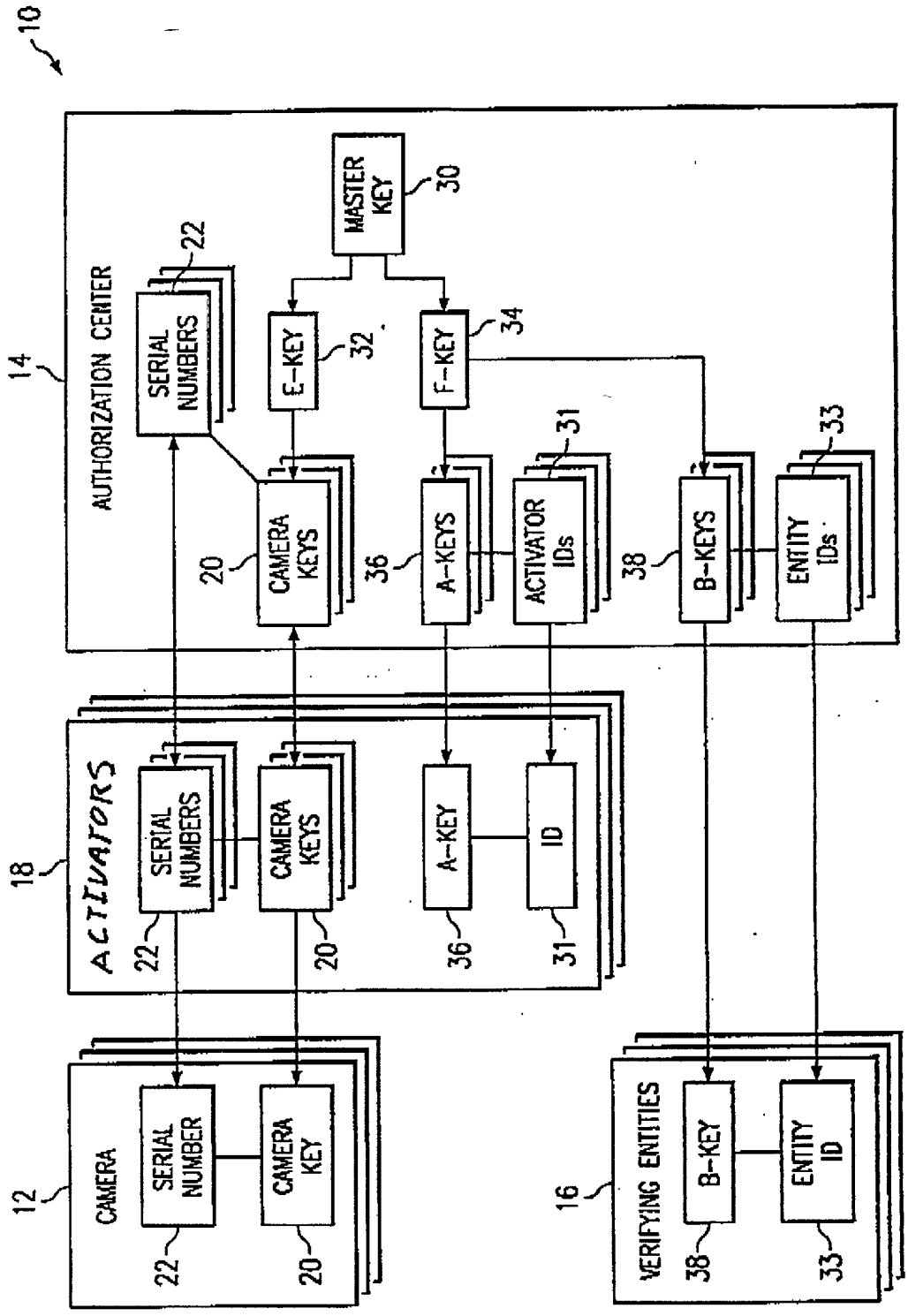

10
AUTHORIZATION CENTER
14
MASTER KEY
30
SERIAL NUMBERS
22
E-KEY
32
F-KEY
34
CAMERA KEYS
20
A-KEYS
36
ACTIVATOR IDs
31
B-KEYS
38
ENTITY IDs
33
ACTIVATORS
18
SERIAL NUMBERS
22
CAMERA KEYS
20
A-KEY
36
ID
31
CAMERA
12
SERIAL NUMBER
22
CAMERA KEY
20
VERIFYING ENTITIES
16
B-KEY
38
ENTITY ID
33

FIG. 2

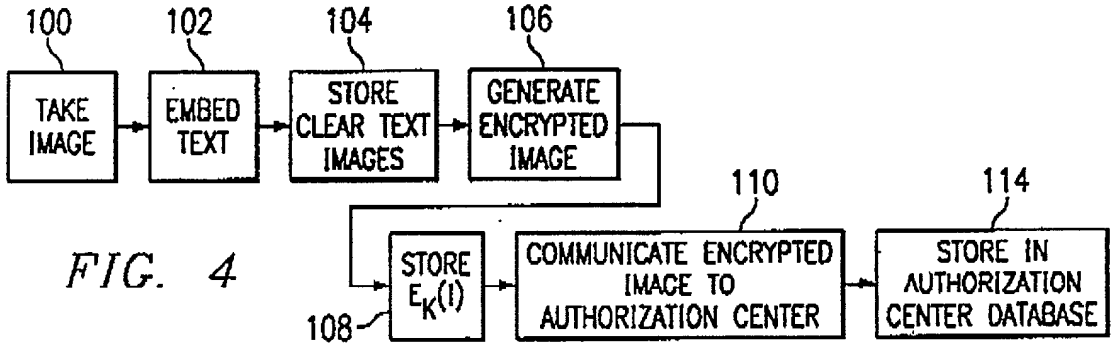


FIG. 4

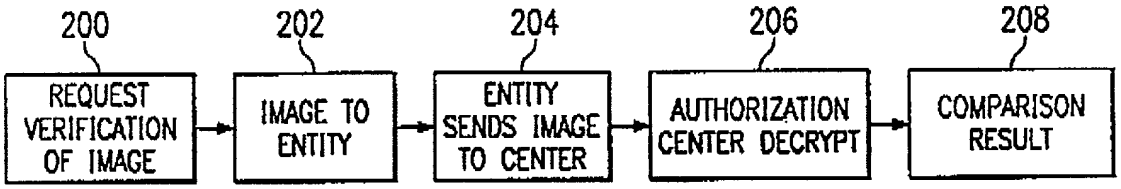


FIG. 5

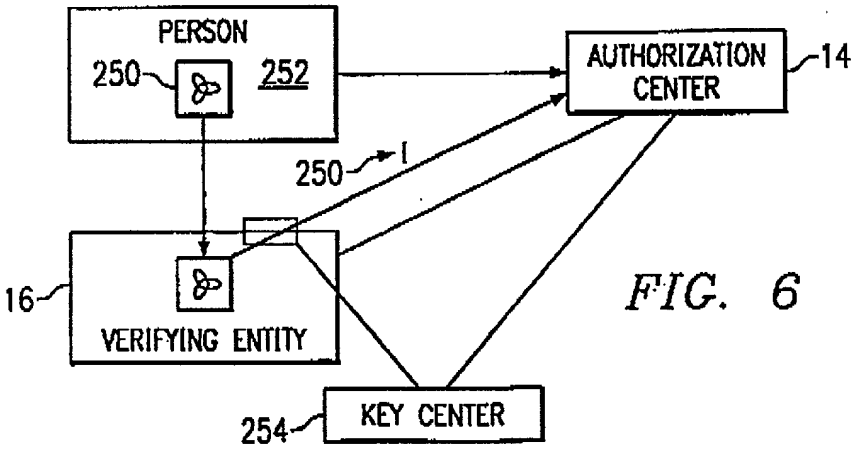


FIG. 6

A4

FIG. 7

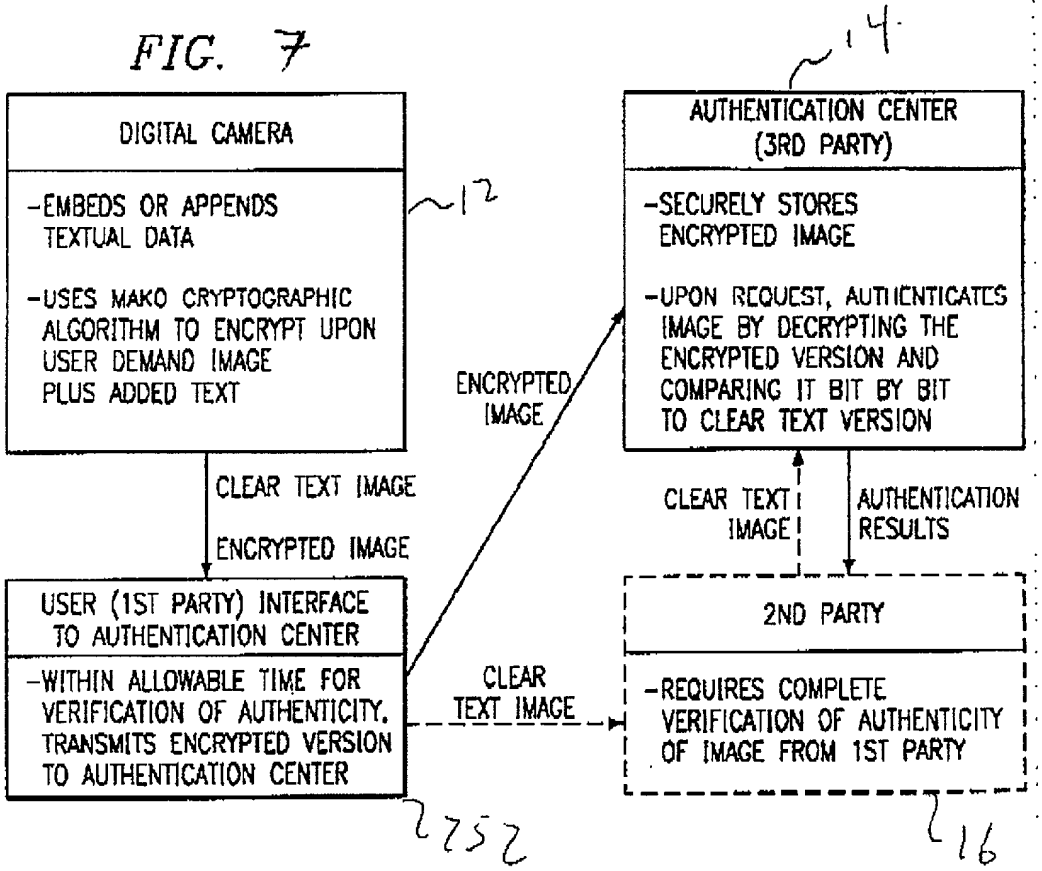
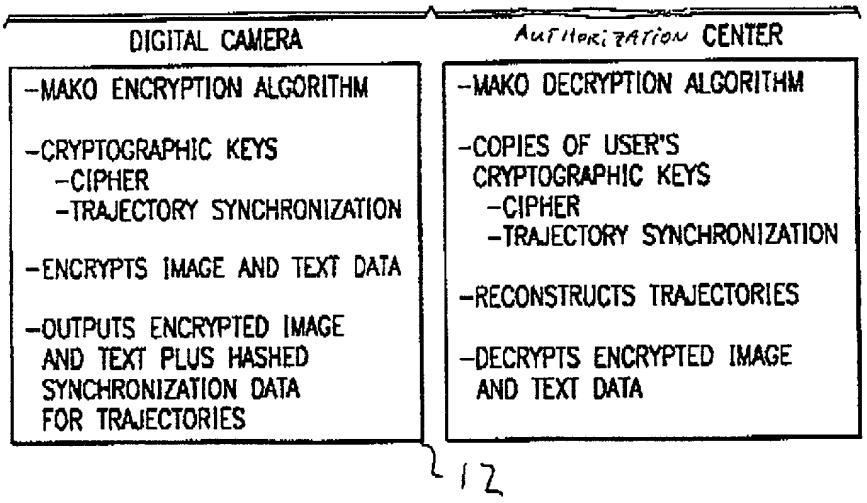

DIGITAL CAMERA
-EMBEDS OR APPENDS TEXTUAL DATA
-USES MAKO CRYPTOGRAPHIC ALGORITHM TO ENCRYPT UPON USER DEMAND IMAGE PLUS ADDED TEXT
12
CLEAR TEXT IMAGE
ENCRYPTED IMAGE
USER (1ST PARTY) INTERFACE TO AUTHENTICATION CENTER
-WITHIN ALLOWABLE TIME FOR VERIFICATION OF AUTHENTICITY, TRANSMITS ENCRYPTED VERSION TO AUTHENTICATION CENTER
752
ENCRYPTED IMAGE
CLEAR TEXT IMAGE
AUTHENTICATION CENTER (3RD PARTY)
-SECURELY STORES ENCRYPTED IMAGE
-UPON REQUEST, AUTHENTICATES IMAGE BY DECRYPTING THE ENCRYPTED VERSION AND COMPARING IT BIT BY BIT TO CLEAR TEXT VERSION
14
CLEAR TEXT IMAGE
AUTHENTICATION RESULTS
2ND PARTY
-REQUIRES COMPLETE VERIFICATION OF AUTHENTICITY OF IMAGE FROM 1ST PARTY
16

FIG. 8


DIGITAL CAMERA
-MAKO ENCRYPTION ALGORITHM
-CRYPTOGRAPHIC KEYS
-CIPHER
-TRAJECTORY SYNCHRONIZATION
-ENCRYPTS IMAGE AND TEXT DATA
-OUTPUTS ENCRYPTED IMAGE AND TEXT PLUS HASHED SYNCHRONIZATION DATA FOR TRAJECTORIES
12
AUTHORIZATION CENTER
-MAKO DECRYPTION ALGORITHM
-COPIES OF USER'S CRYPTOGRAPHIC KEYS
-CIPHER
-TRAJECTORY SYNCHRONIZATION
-RECONSTRUCTS TRAJECTORIES
-DECRYPTS ENCRYPTED IMAGE AND TEXT DATA

A4

FIG. 9

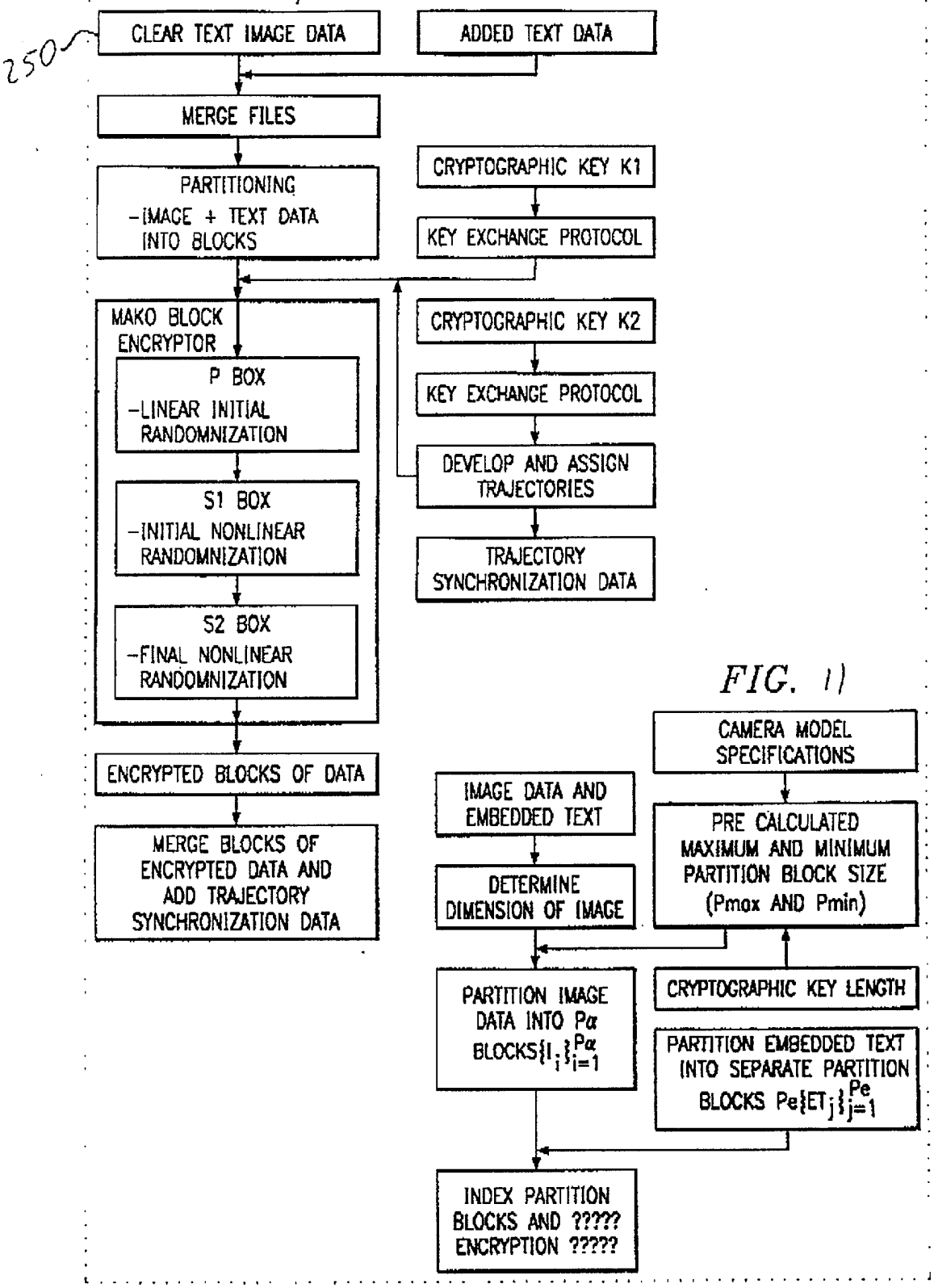


FIG. 11

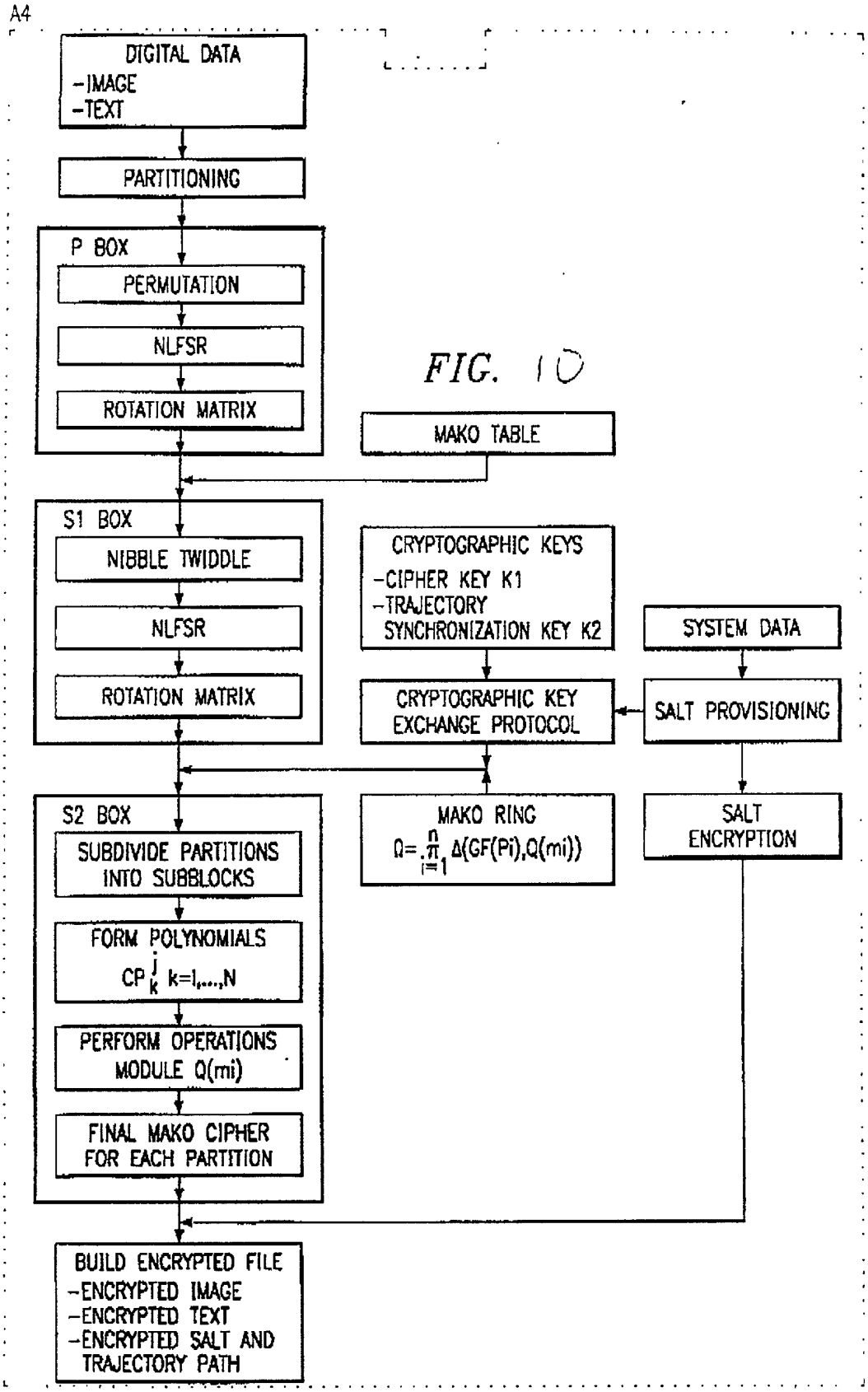
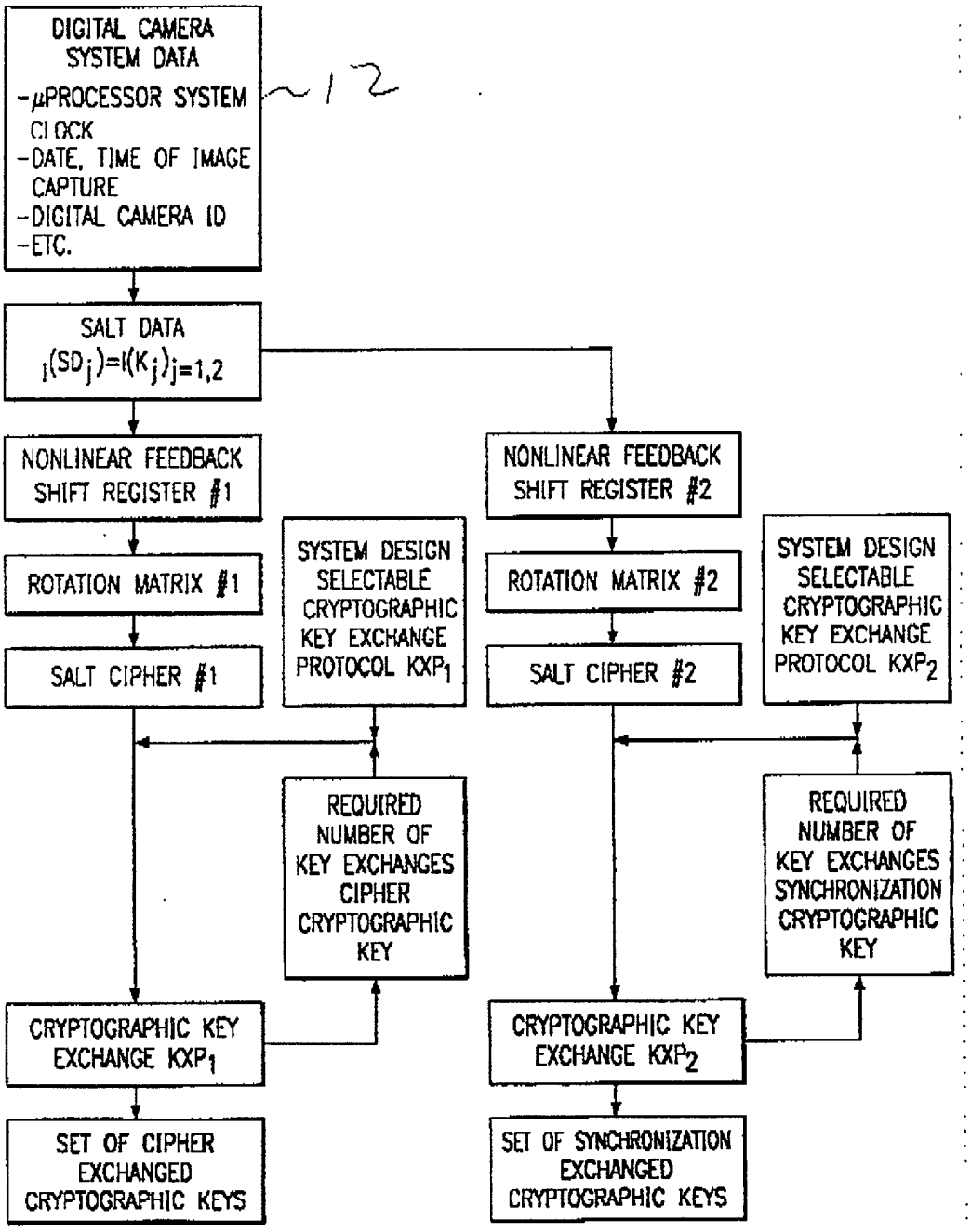

A4
DIGITAL DATA
-IMAGE
-TEXT
PARTITIONING
P BOX
PERMUTATION
NLFSR
ROTATION MATRIX
MAKO TABLE
S1 BOX
NIBBLE TWIDDLE
NLFSR
ROTATION MATRIX
CRYPTOGRAPHIC KEYS
-CIPHER KEY K1
-TRAJECTORY SYNCHRONIZATION KEY K2
SYSTEM DATA
CRYPTOGRAPHIC KEY EXCHANGE PROTOCOL
SALT PROVISIONING
S2 BOX
SUBDIVIDE PARTITIONS INTO SUBBLOCKS
FORM POLYNOMIALS
CP j k k=1,...,N
PERFORM OPERATIONS MODULE Q(mi)
FINAL MAKO CIPHER FOR EACH PARTITION
MAKO RING
Q=∏ i=1 n Δ(GF(Pi),Q(mi))
SALT ENCRYPTION
BUILD ENCRYPTED FILE
-ENCRYPTED IMAGE
-ENCRYPTED TEXT
-ENCRYPTED SALT AND TRAJECTORY PATH

FIG. 10

A4

FIG. 12


DIGITAL CAMERA SYSTEM DATA
-μPROCESSOR SYSTEM CLOCK
-DATE, TIME OF IMAGE CAPTURE
-DIGITAL CAMERA ID
-ETC.
12
SALT DATA
$_1(SD_j)=I(K_j)_{j=1,2}$
NONLINEAR FEEDBACK SHIFT REGISTER #1
ROTATION MATRIX #1
SALT CIPHER #1
SYSTEM DESIGN SELECTABLE CRYPTOGRAPHIC KEY EXCHANGE PROTOCOL KXP_1
REQUIRED NUMBER OF KEY EXCHANGES CIPHER CRYPTOGRAPHIC KEY
CRYPTOGRAPHIC KEY EXCHANGE KXP_1
SET OF CIPHER EXCHANGED CRYPTOGRAPHIC KEYS
NONLINEAR FEEDBACK SHIFT REGISTER #2
ROTATION MATRIX #2
SALT CIPHER #2
SYSTEM DESIGN SELECTABLE CRYPTOGRAPHIC KEY EXCHANGE PROTOCOL KXP_2
REQUIRED NUMBER OF KEY EXCHANGES SYNCHRONIZATION CRYPTOGRAPHIC KEY
CRYPTOGRAPHIC KEY EXCHANGE KXP_2
SET OF SYNCHRONIZATION EXCHANGED CRYPTOGRAPHIC KEYS

A4

FIG. 13

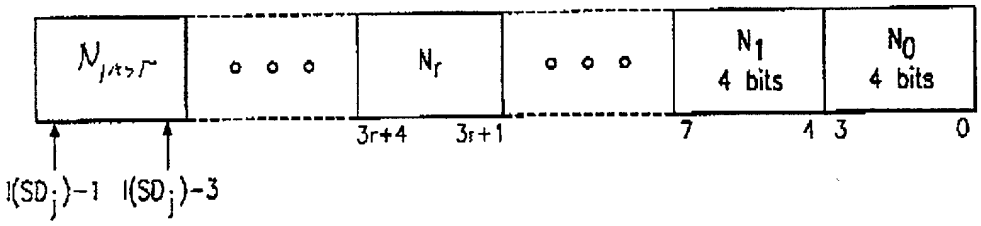
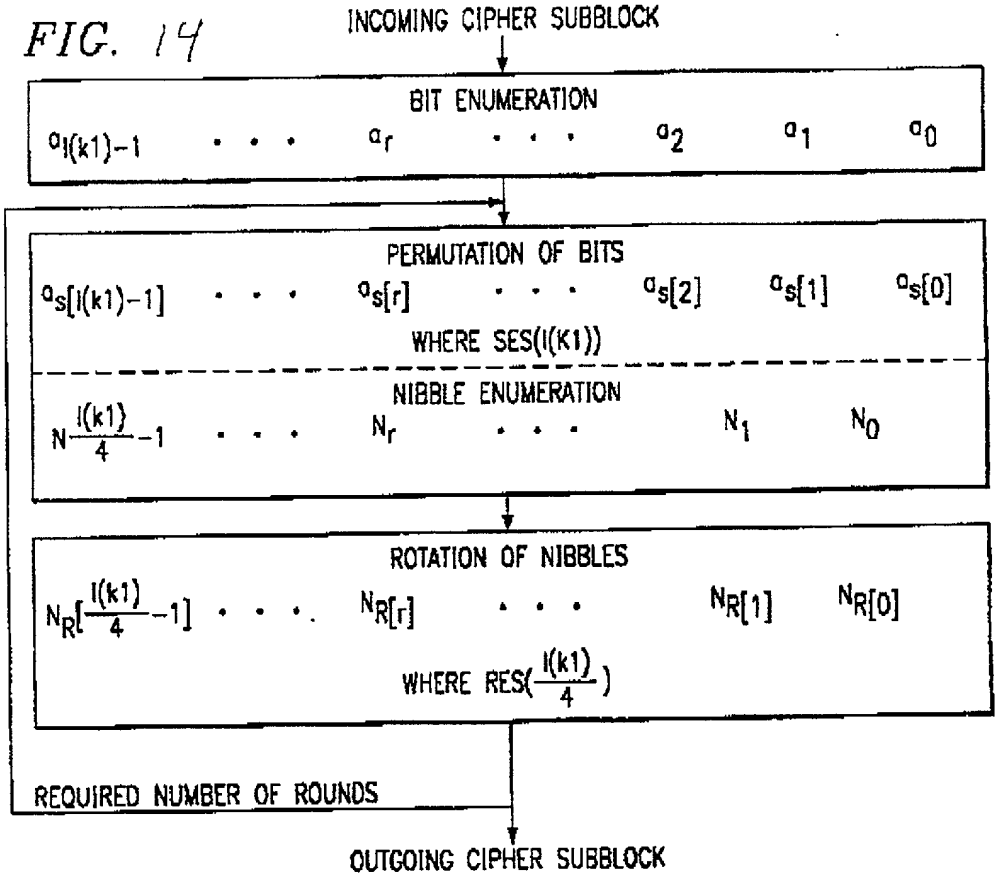


FIG. 14



A4

FIG. 15

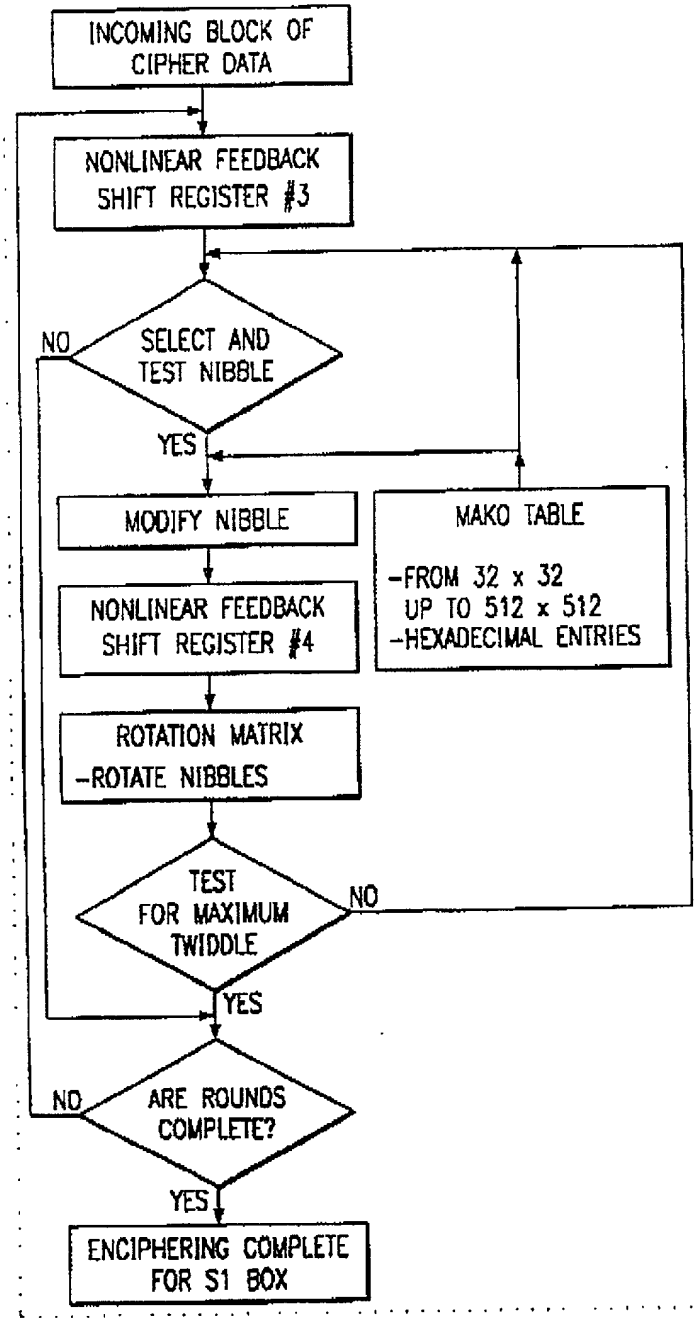
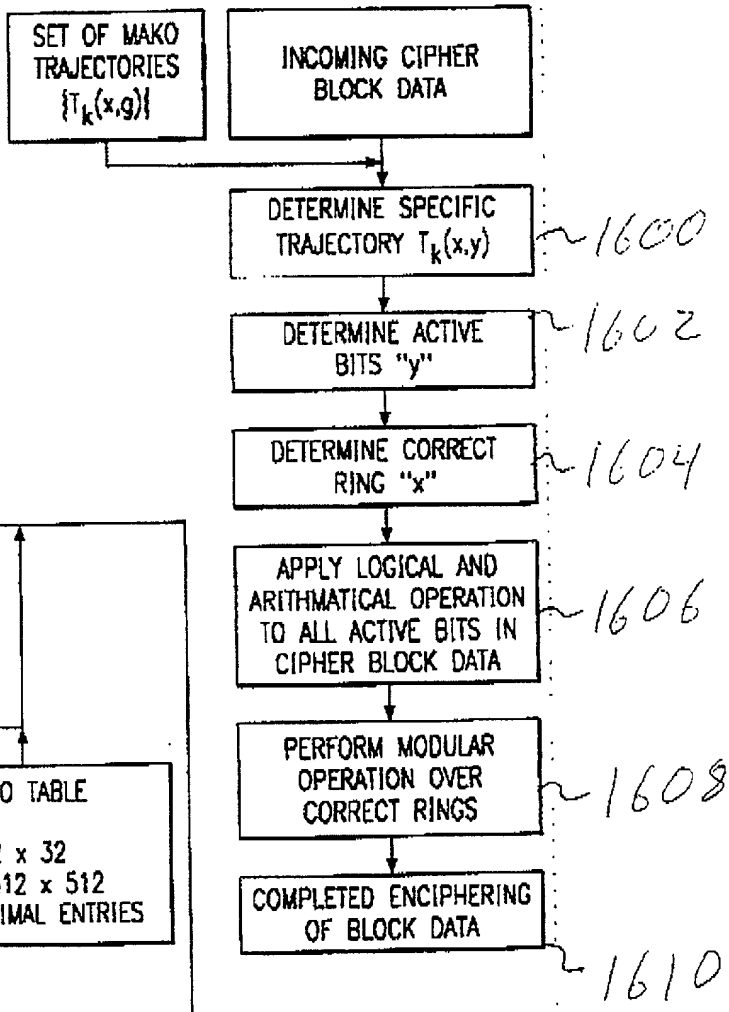


FIG. 16



A4

FIG. 17

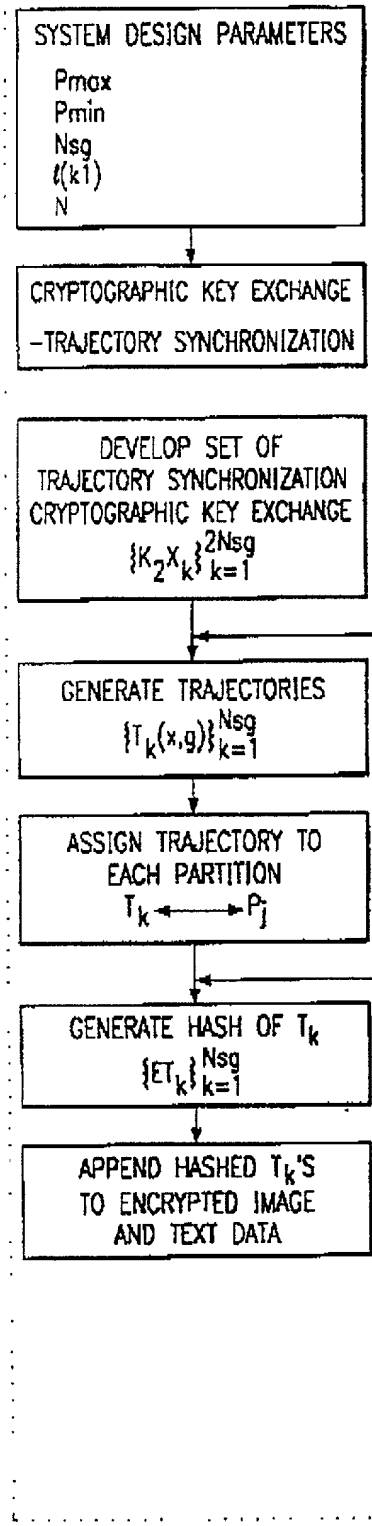
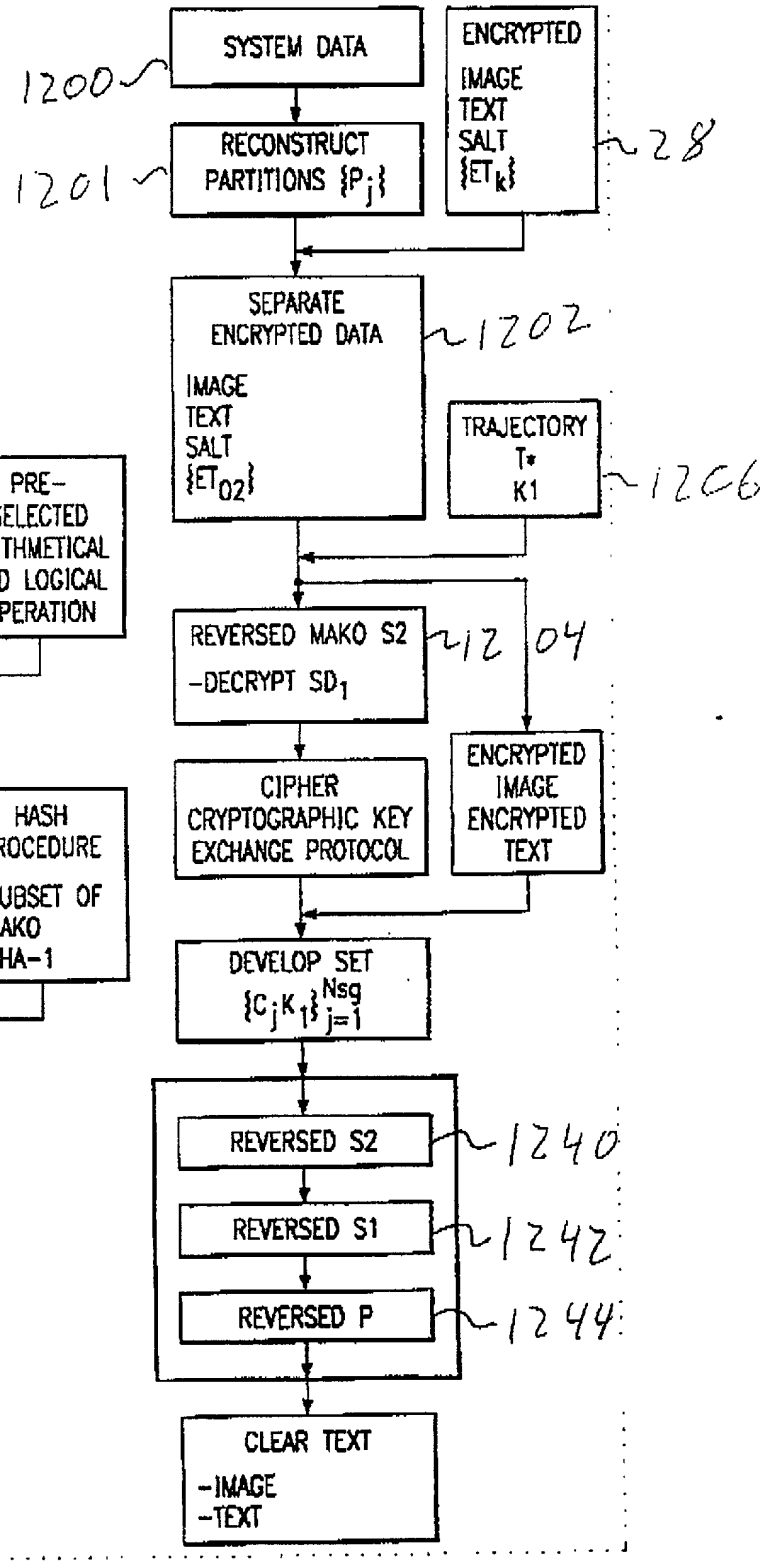


FIG. 18



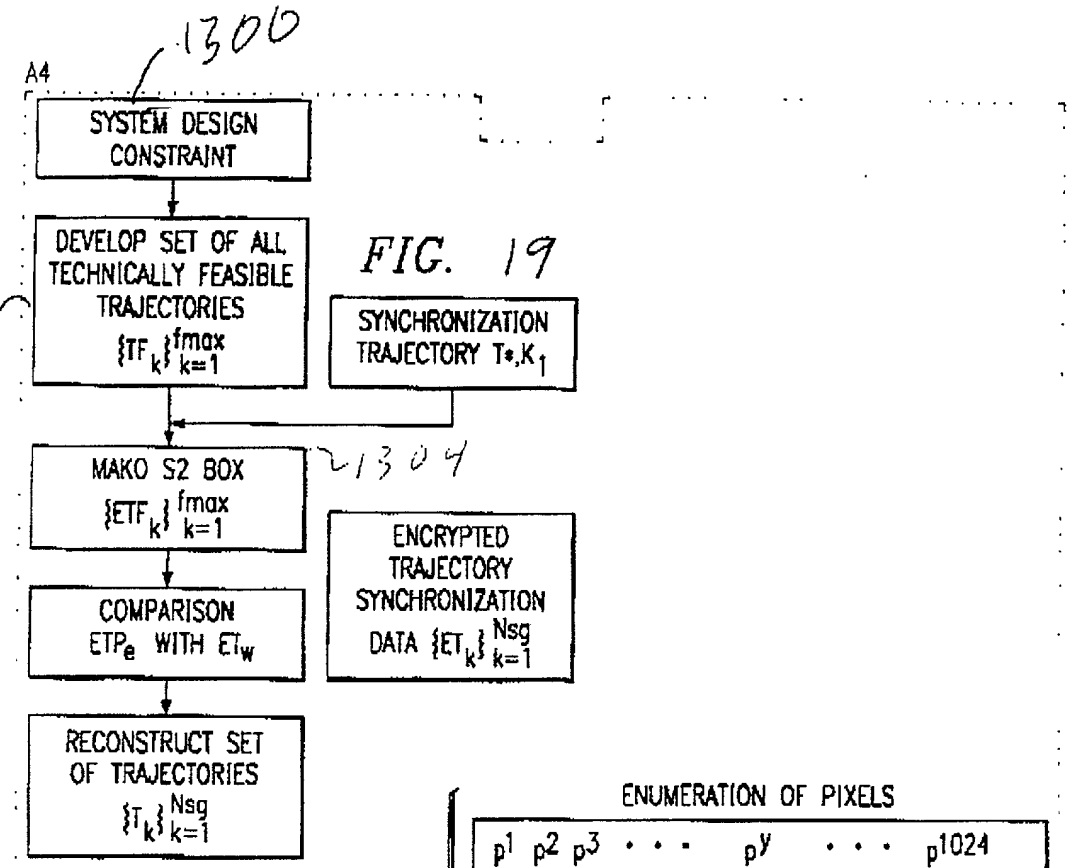


FIG. 19

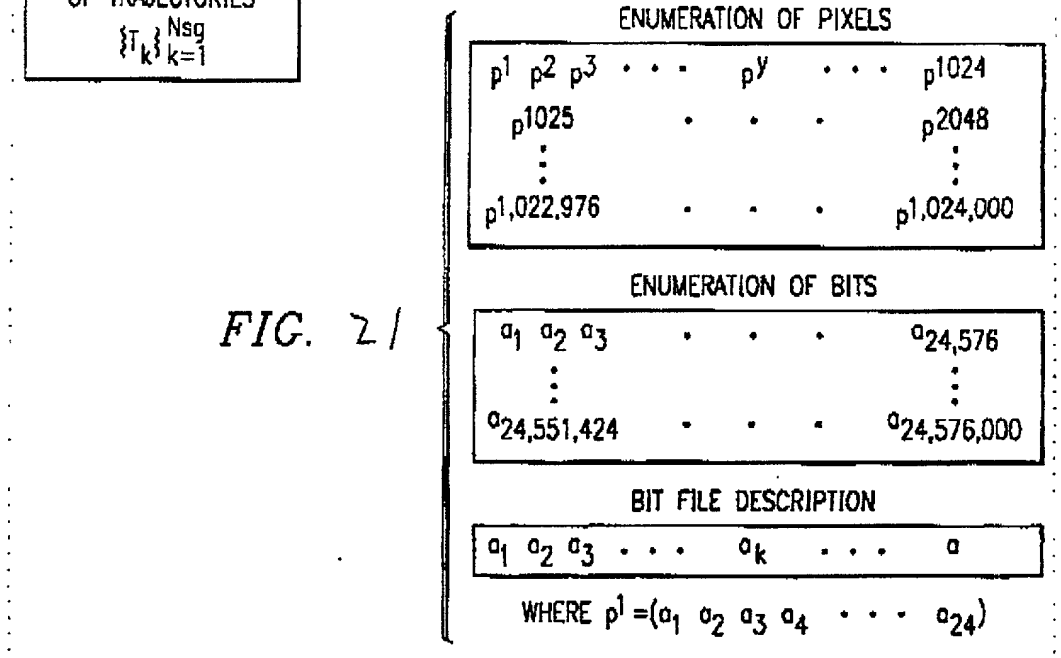


FIG. 21

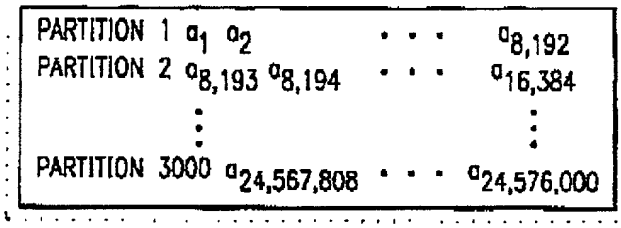


FIG. 22

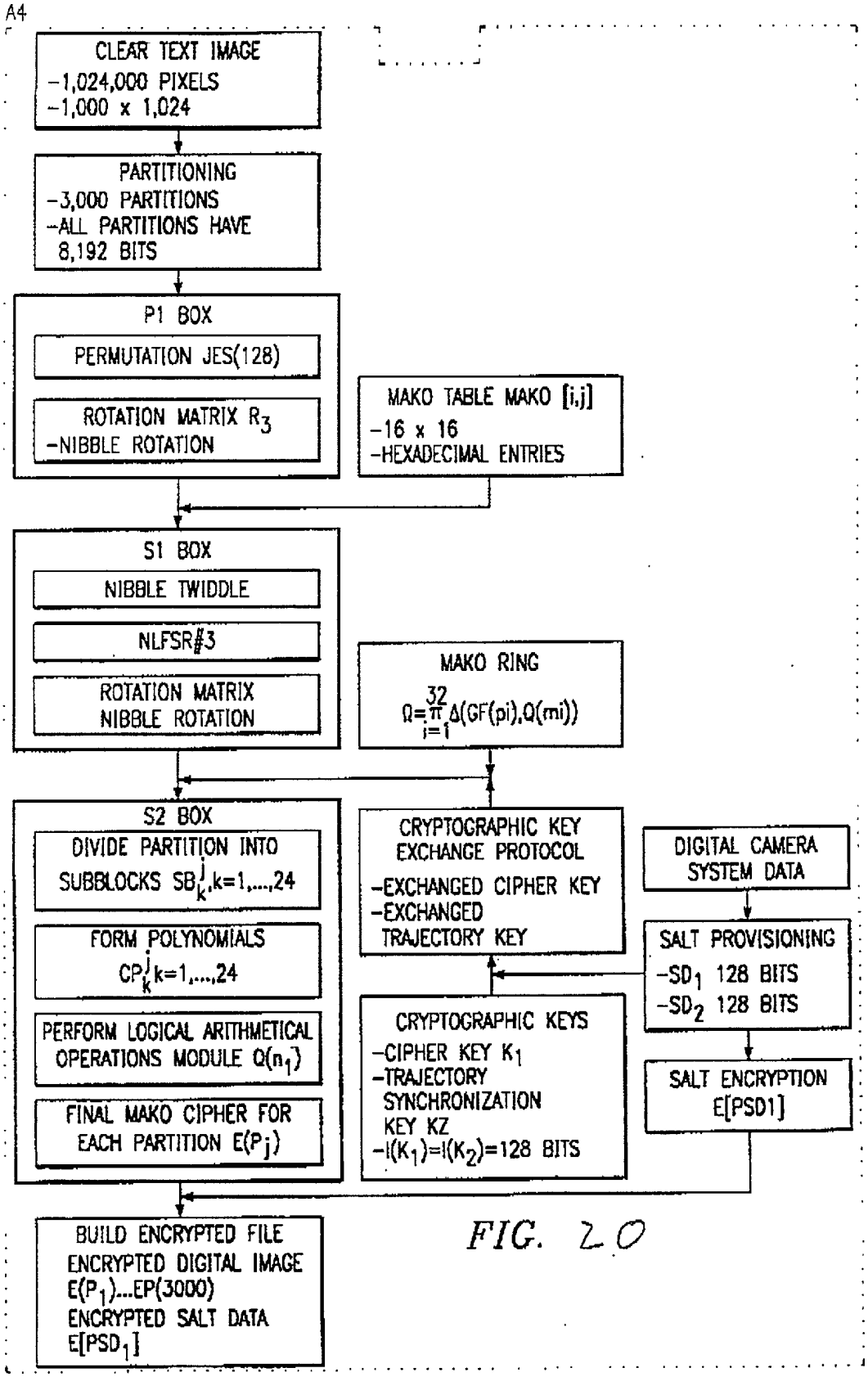
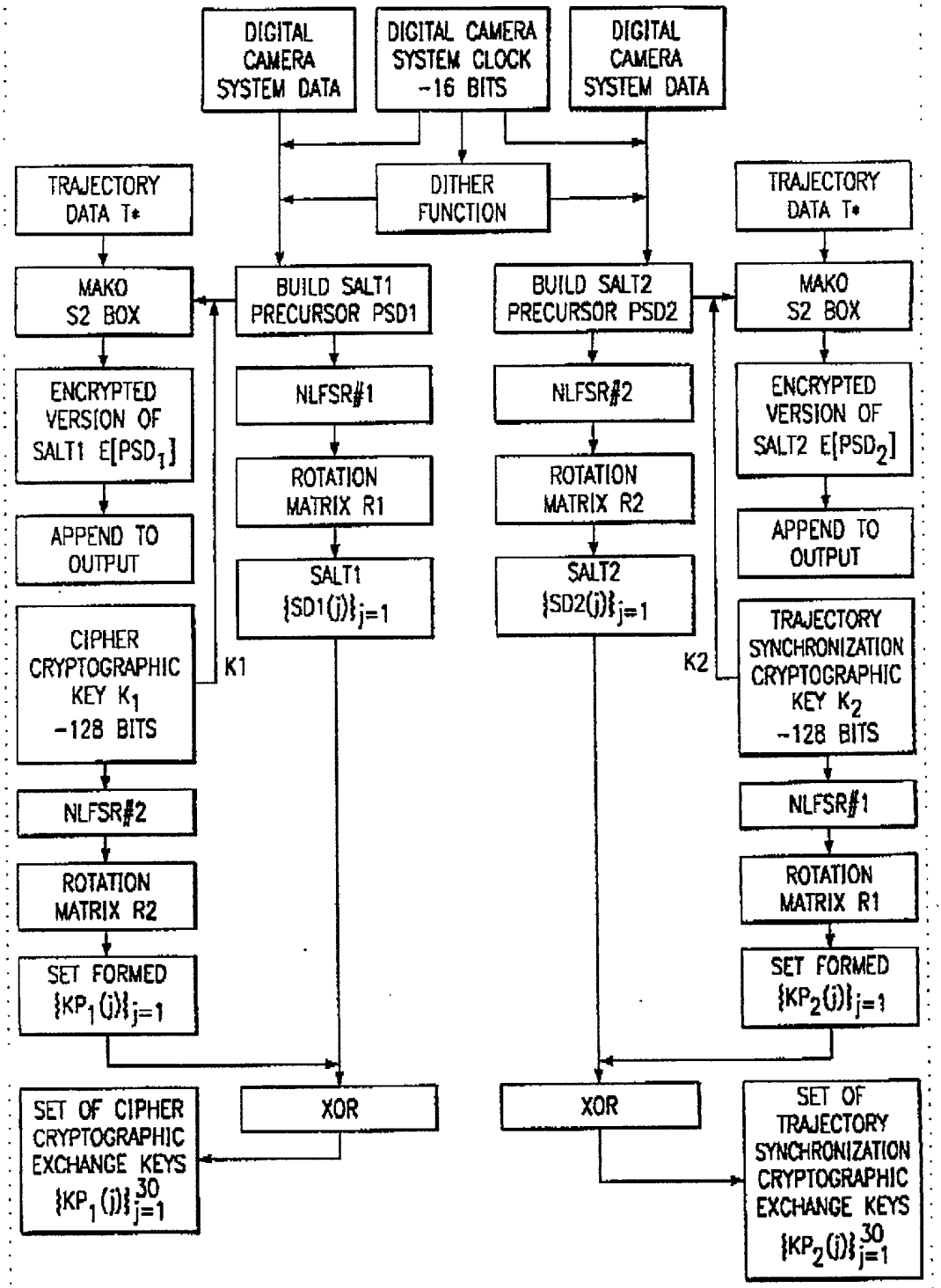

A4
CLEAR TEXT IMAGE
-1,024,000 PIXELS
-1,000 x 1,024
PARTITIONING
-3,000 PARTITIONS
-ALL PARTITIONS HAVE 8,192 BITS
P1 BOX
PERMUTATION JES(128)
ROTATION MATRIX R_3
-NIBBLE ROTATION
MAKO TABLE MAKO [i,j]
-16 x 16
-HEXADECIMAL ENTRIES
S1 BOX
NIBBLE TWIDDLE
NLFSR#3
ROTATION MATRIX
NIBBLE ROTATION
MAKO RING
$\Omega=\frac{32}{\pi}_{i=1}\Delta(GF(pi),Q(mi))$
S2 BOX
DIVIDE PARTITION INTO SUBBLOCKS SB^j_k,k=1,...,24
FORM POLYNOMIALS CP^j_k,k=1,...,24
PERFORM LOGICAL ARITHMETICAL OPERATIONS MODULE $Q(n_1)$
FINAL MAKO CIPHER FOR EACH PARTITION $E(P_j)$
CRYPTOGRAPHIC KEY EXCHANGE PROTOCOL
-EXCHANGED CIPHER KEY
-EXCHANGED TRAJECTORY KEY
CRYPTOGRAPHIC KEYS
-CIPHER KEY K_1
-TRAJECTORY SYNCHRONIZATION KEY KZ
$-l(K_1)=l(K_2)=128$ BITS
DIGITAL CAMERA SYSTEM DATA
SALT PROVISIONING
$-SD_1$ 128 BITS
$-SD_2$ 128 BITS
SALT ENCRYPTION E[PSD1]
BUILD ENCRYPTED FILE
ENCRYPTED DIGITAL IMAGE
$E(P_1)...EP(3000)$
ENCRYPTED SALT DATA
$E[PSD_1]$

FIG. 20

A4

FIG. 23


DIGITAL CAMERA SYSTEM DATA
DIGITAL CAMERA SYSTEM CLOCK -16 BITS
DIGITAL CAMERA SYSTEM DATA
TRAJECTORY DATA T*
DITHER FUNCTION
TRAJECTORY DATA T*
MAKO S2 BOX
BUILD SALT1 PRECURSOR PSD1
BUILD SALT2 PRECURSOR PSD2
MAKO S2 BOX
ENCRYPTED VERSION OF SALT1 E[PSD1]
NLFSR#1
NLFSR#2
ENCRYPTED VERSION OF SALT2 E[PSD2]
APPEND TO OUTPUT
ROTATION MATRIX R1
ROTATION MATRIX R2
APPEND TO OUTPUT
SALT1 {SD1(j)}j=1
SALT2 {SD2(j)}j=1
CIPHER CRYPTOGRAPHIC KEY K1 -128 BITS
K1
K2
TRAJECTORY SYNCHRONIZATION CRYPTOGRAPHIC KEY K2 -128 BITS
NLFSR#2
NLFSR#1
ROTATION MATRIX R2
ROTATION MATRIX R1
SET FORMED {KP1(j)}j=1
SET FORMED {KP2(j)}j=1
XOR
XOR
SET OF CIPHER CRYPTOGRAPHIC EXCHANGE KEYS {KP1(j)}j=1 30
SET OF TRAJECTORY SYNCHRONIZATION CRYPTOGRAPHIC EXCHANGE KEYS {KP2(j)}j=1 30

A4

FIG. 35

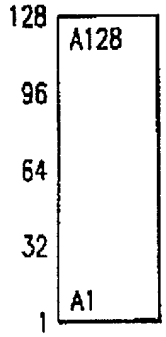


FIG. 36

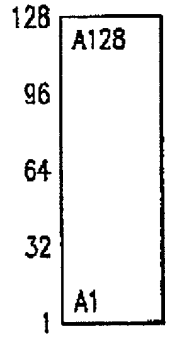


FIG. 33

CURRENT	NEW
R0	R23
R1	R24
R2	R25
R3	R26
R4	R27
R5	R28
R6	R29
R7	R30
R9	R31
R8	R0
R10	R1
R11	R2
R12	R3
R13	R4
R14	R5
R15	R6
R16	R7
R17	R8
R18	R9
R19	R10
R20	R11
R21	R12
R22	R13
R23	R14
R24	R15
R25	R16
R26	R17
R27	R18
R28	R19
R29	R20
R30	R21
R31	R22

FIG. 34

CURRENT	NEW
R0	R13
R1	R14
R2	R15
R3	R16
R4	R17
R5	R18
R6	R19
R7	R20
R9	R21
R8	R22
R10	R23
R11	R24
R12	R25
R13	R26
R14	R27
R15	R28
R16	R29
R17	R30
R18	R31
R19	R0
R20	R1
R21	R2
R22	R3
R23	R4
R24	R5
R25	R6
R26	R7
R27	R8
R28	R9
R29	R10
R30	R11
R31	R12

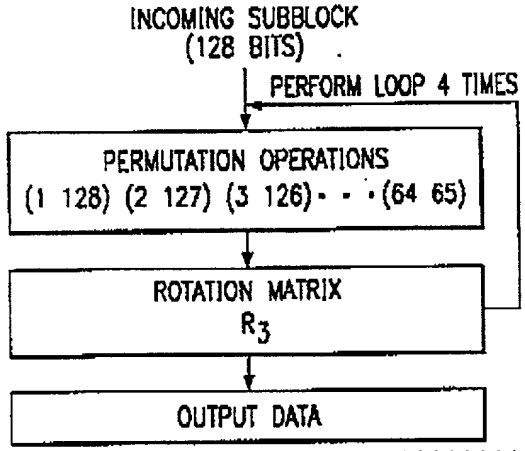


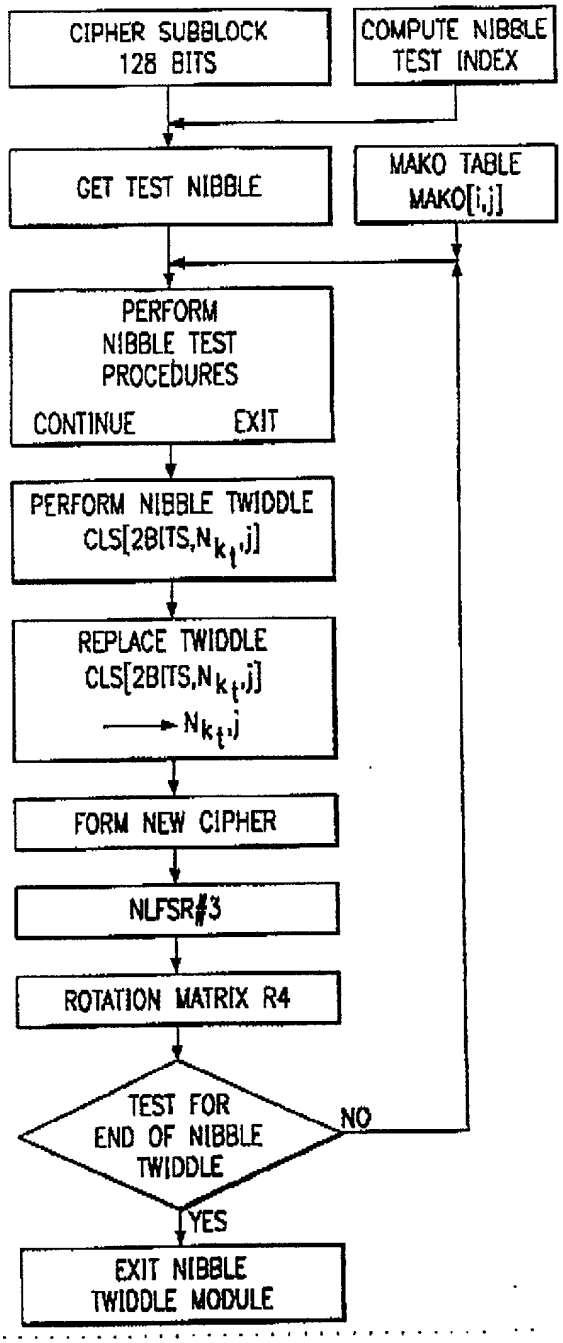
FIG. 24

A4

FIG. 25

CURRENT	NEW
R0	R15
R1	R14
R2	R13
R3	R12
R4	R11
R5	R10
R6	R9
R7	R8
R9	R22
R10	R21
R11	R20
R12	R19
R13	R18
R14	R17
R15	R16
R16	R31
R17	R30
R18	R29
R19	R28
R20	R27
R21	R26
R22	R25
R23	R24
R24	R7
R25	R6
R26	R5
R27	R4
R28	R3
R29	R2
R30	R1
R31	R0

FIG. 26



A4

FIG. 27

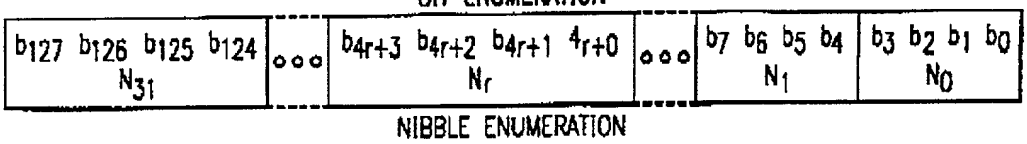


FIG. 32

MAKOTABLE[m_{ij}]=

0f	1f	2f	3f	4f	5f	6f	7f	8f	9f	af	bf	cf	df	ef	
1e	2e	3e	4e	5e	6e	7e	8e	9e	ae	be	ce	de	ee	fe	0
2d	3d	4d	5d	6d	7d	8d	9d	ad	bd	cd	dd	ed	fd	0d	1
3c	4c	5c	6c	7c	8c	9c	ac	bc	cc	dc	ec	fc	0c	1c	2
4b	5b	6b	7b	8b	9b	ab	bb	cb	db	eb	fb	0b	1b	2b	3
5a	6a	7a	8a	9a	aa	ba	ca	da	ea	fa	0a	1a	2a	3a	4
69	79	89	99	a9	b9	c9	d9	e9	f9	09	19	29	39	49	5
78	88	98	a8	b8	c8	d8	e8	f8	08	18	28	38	48	58	6
87	97	a7	b7	c7	d7	e7	f7	07	17	27	37	47	57	67	7
96	a6	b6	c6	d6	e6	f6	06	16	26	36	46	56	66	76	8
a5	b5	c5	d5	e5	f5	05	15	25	35	45	55	65	75	85	9
b4	c4	d4	e4	f4	04	14	24	34	44	54	64	74	84	94	a
c3	d3	e3	f3	03	13	23	33	43	53	63	73	83	93	a3	b
d2	c2	f2	02	12	22	32	42	52	62	72	82	92	a2	b2	c
e1	f1	01	11	21	31	41	51	61	71	81	91	a1	b1	c1	d
e0	00	10	20	30	40	50	60	70	80	90	a0	b0	c0	d0	f0

A4

FIG. 28

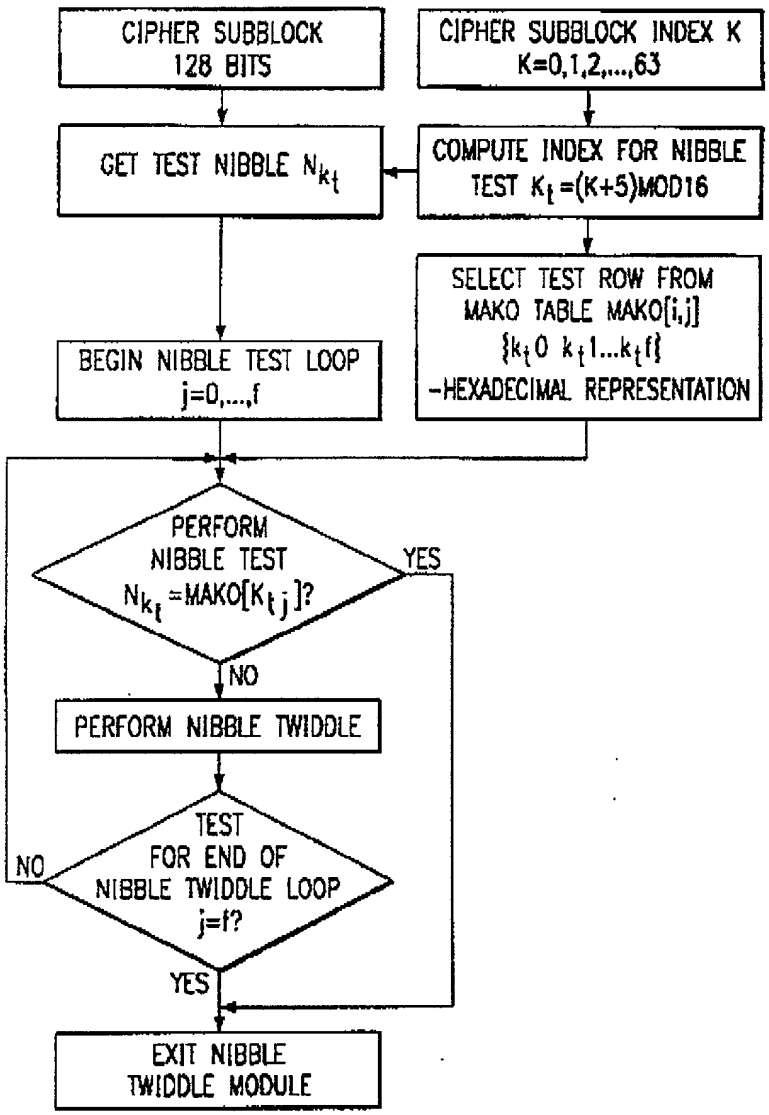


FIG. 29

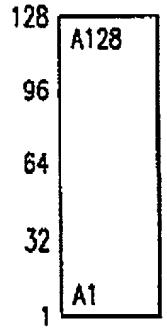
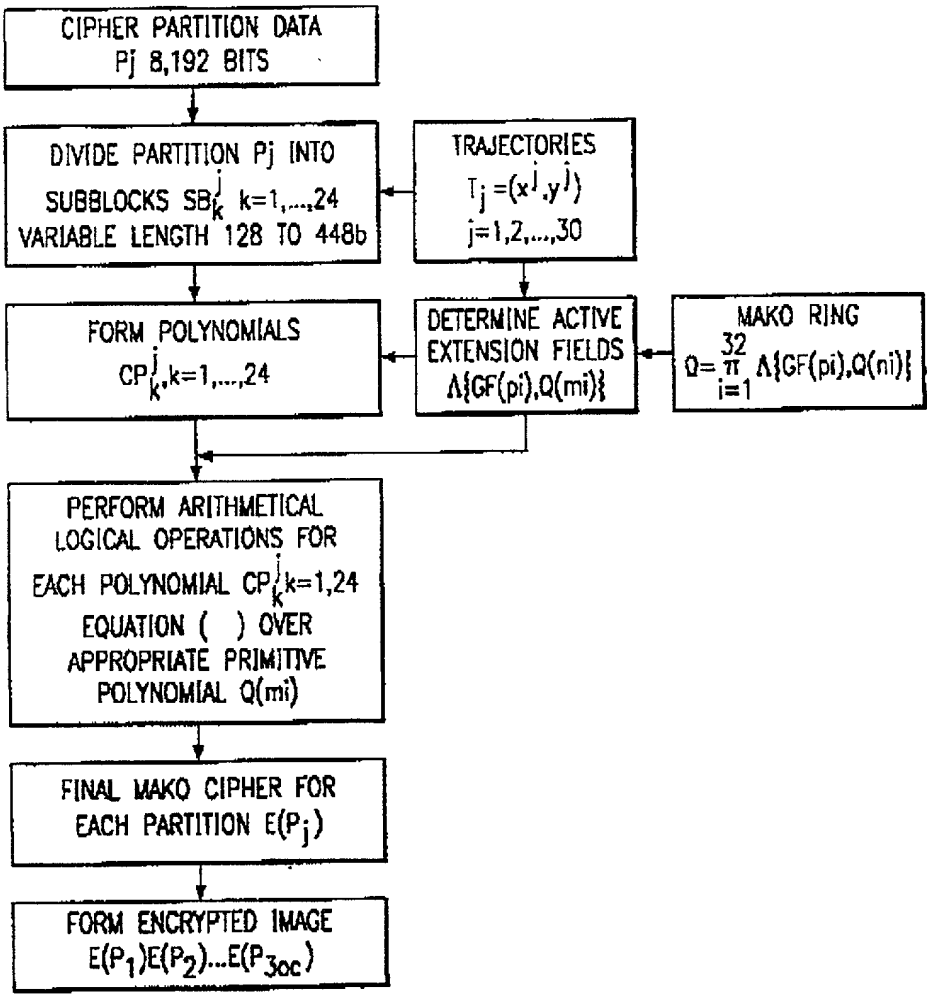


FIG. 37

CURRENT	NEW
R0	R15
R1	R14
R2	R13
R3	R12
R4	R11
R5	R10
R6	R9
R7	R8
R9	R22
R10	R21
R11	R20
R12	R19
R13	R18
R14	R17
R15	R16
R16	R31
R17	R30
R18	R29
R19	R28
R20	R27
R21	R26
R22	R25
R23	R24
R24	R7
R25	R6
R26	R5
R27	R4
R28	R3
R29	R2
R30	R1
R31	R0

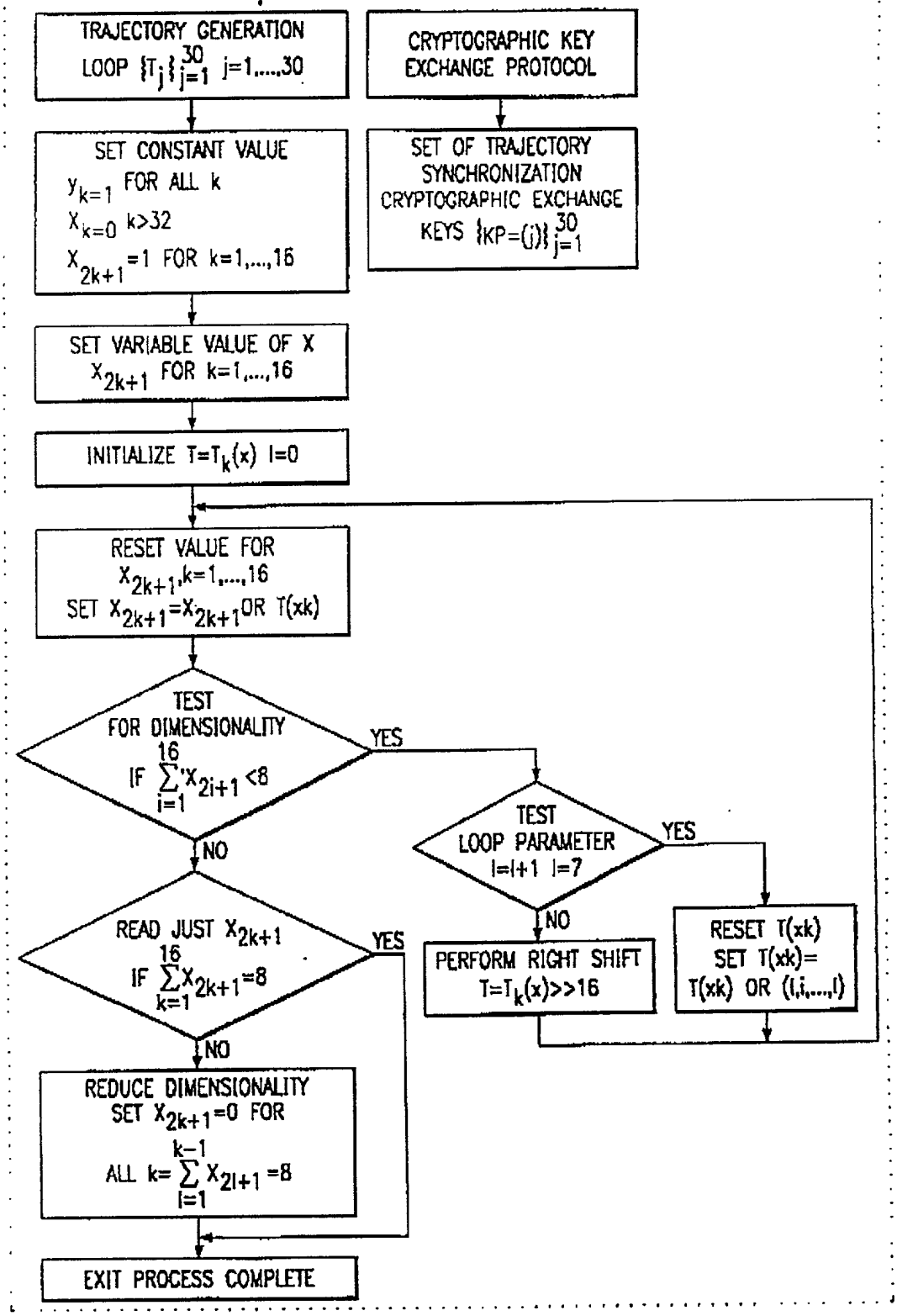
A4

FIG. 30


CIPHER PARTITION DATA
Pj 8,192 BITS
DIVIDE PARTITION Pj INTO
SUBBLOCKS SB_k^j k=1,...,24
VARIABLE LENGTH 128 TO 448b
TRAJECTORIES
$T_j=(x^j,y^j)$
j=1,2,...,30
FORM POLYNOMIALS
CP_k^j,k=1,...,24
DETERMINE ACTIVE
EXTENSION FIELDS
Λ{GF(pi),Q(mi)}
MAKO RING
$Q=\frac{32}{\pi}_{i=1}\Lambda\{GF(pi),Q(ni)\}$
PERFORM ARITHMETICAL
LOGICAL OPERATIONS FOR
EACH POLYNOMIAL CP_k^jk=1,24
EQUATION ( ) OVER
APPROPRIATE PRIMITIVE
POLYNOMIAL Q(mi)
FINAL MAKO CIPHER FOR
EACH PARTITION $E(P_j)$
FORM ENCRYPTED IMAGE
$E(P_1)E(P_2)...E(P_{30c})$

A4

FIG. 31


TRAJECTORY GENERATION
LOOP $\{T_j\}_{j=1}^{30}$ j=1,...,30
CRYPTOGRAPHIC KEY EXCHANGE PROTOCOL
SET CONSTANT VALUE
$y_{k=1}$ FOR ALL k
$X_{k=0}$ k>32
X_{2k+1}=1 FOR k=1,...,16
SET OF TRAJECTORY SYNCHRONIZATION CRYPTOGRAPHIC EXCHANGE KEYS $\{KP=\{j\}\}_{j=1}^{30}$
SET VARIABLE VALUE OF X
X_{2k+1} FOR k=1,...,16
INITIALIZE T=$T_k(x)$ I=0
RESET VALUE FOR
X_{2k+1},k=1,...,16
SET $X_{2k+1}=X_{2k+1}$ OR T(xk)
TEST FOR DIMENSIONALITY
IF $\sum_{i=1}^{16} X_{2i+1}$ <8
YES
NO
TEST LOOP PARAMETER
I=I+1 I=7
YES
NO
RESET T(xk)
SET T(xk)=
T(xk) OR (I,I,...,I)
PERFORM RIGHT SHIFT
T=$T_k(x)$>>16
READ JUST X_{2k+1}
IF $\sum_{k=1}^{16} X_{2k+1}$=8
YES
NO
REDUCE DIMENSIONALITY
SET X_{2k+1}=0 FOR
ALL k= $\sum_{I=1}^{k-1} X_{2I+1}$ =8
EXIT PROCESS COMPLETE